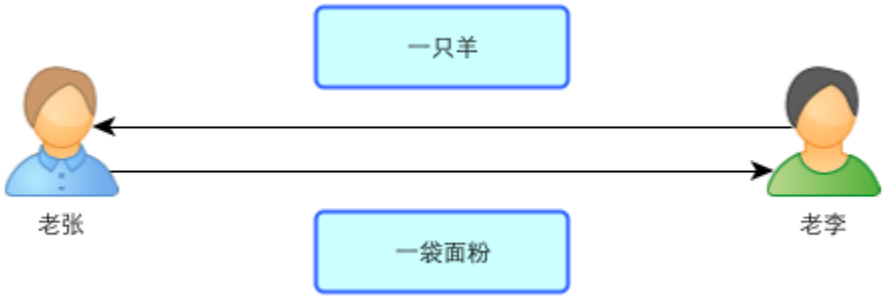
问题的提出

我们先从比特币产生的动机开始。

以物易物的比特村

话说在这个世界上，有一个叫比特村的小村庄，村庄共有几百户人家。这个村庄几乎与世隔绝，过着自给自足的生活。由于没有大规模贸易，比特村村民一直过着以物易物的生活，也就是说村民之间并没有使用统一的货币，互相间的贸易基本上就是老张家拿一袋面粉换老李家一只羊，王大嫂拿一筐野果换刘大婶两尺布。村民们一直就这么纯朴的生活着。

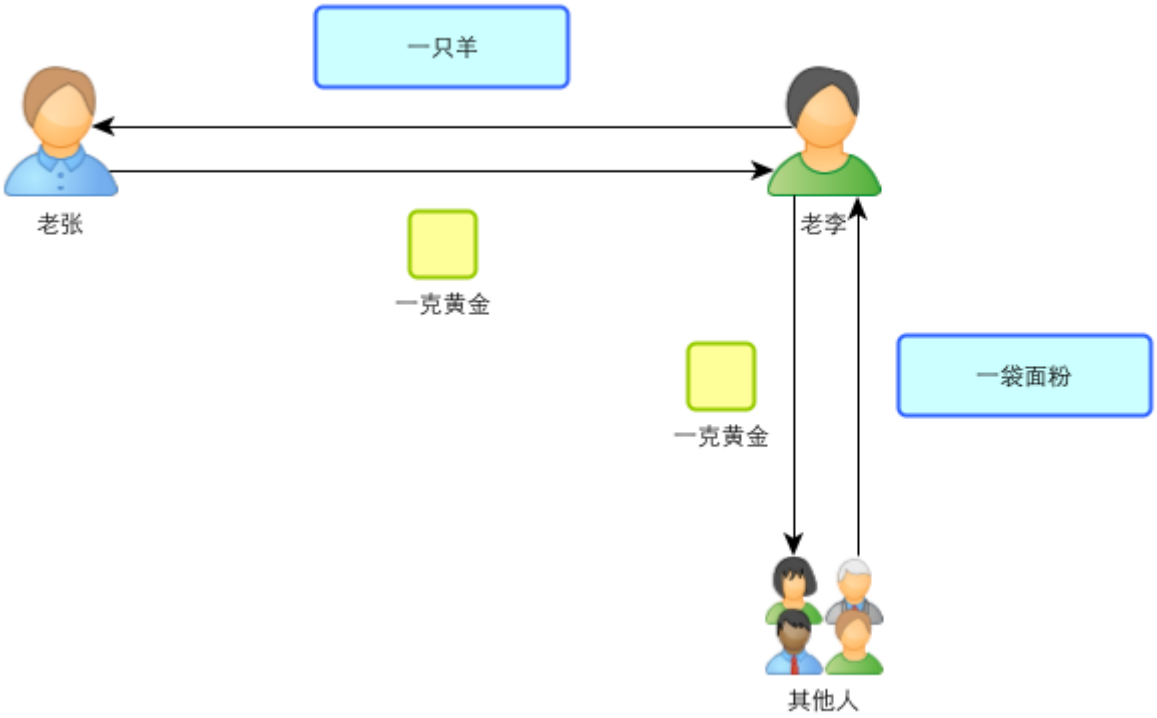


实物货币

终于有一天，村民觉得一直这样以物易物实在太不方便了，于是村子全员开会，讨论如何解决这个问题。有人提议，以便于分割且稀有的东西，例如黄金，作为一般等价物，把其它物品和黄金的对应关系编成一张表格，例如一克黄金对应一只羊，一克黄金对应一袋面粉等等，此时老张再也不用扛着一袋面粉气喘吁吁的去老李家换羊了，他只要从家里摸出一克金子，就可以去老李家牵回一只羊，而老李拿着这一克黄金可以从

任何愿意出让面粉的人那里换回一袋面粉，当然也可以换取任何和一克黄金等值的物品。

此时比特村进入了实物货币时代。



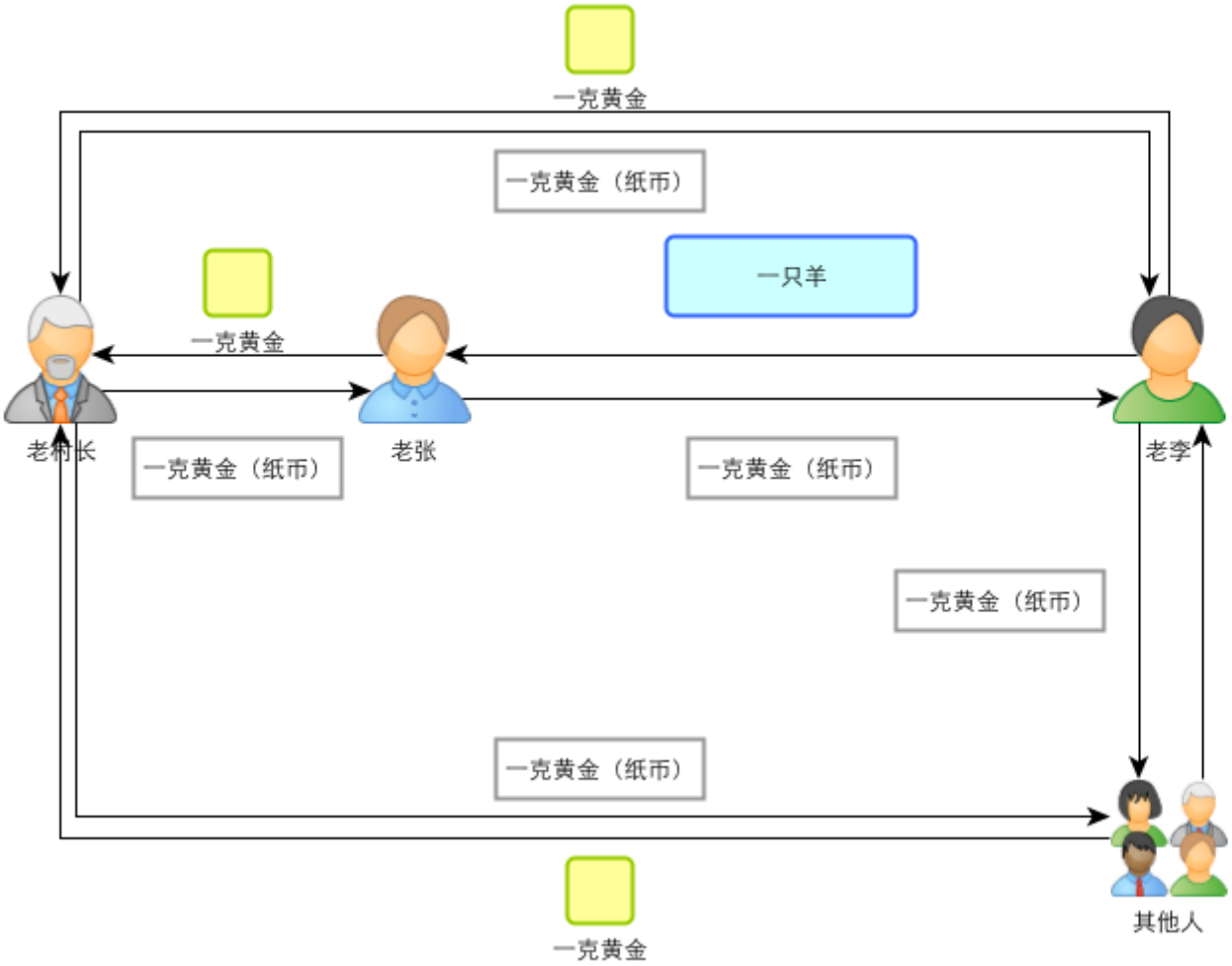
符号货币

好景不长，过了一段时间，实物货币的弊端也出现了。因为比特村附近金矿并不多，开采和冶炼金子太费时费力了。而随着使用，金子总是不断会因为磨损、丢失或有人故意囤积而发生损耗。全村人又一次坐在了一起，开始商讨对策。此时有人说，其实大家也不必一定要真的用黄金啊，随便找张纸，写上“一克黄金”，只要全村人都认同这张纸就等于一克黄金，问题不就解决了。其他人纷纷表示认同，但同时也有了新的问题：真实的黄金是需要开采和冶炼的，金矿有限，开采和冶炼也需要成

本，所以没有人可以短期凭空制造大量的黄金，可写字就不同了，只要我纸够笔够，随便像写多少写多少，那这就变成拼谁家里纸多了，搞不好到时一万张纸才能换一只羊（实际上这就发生了经济学上的通货膨胀）。

大家一想也是啊。不过此时又有人提出了解决方案：这个纸不是谁写都有效，我们只认村里德高望重的老村长写得，大家都认识老村长的字。老村长写一些纸，同时按照各家黄金存量发给大家等量的纸，例如老张家有二百克黄金，老村长就发给老张二百张写着“一克黄金”的纸，同时将老张家的黄金拿走作为抵押。就这样，老村长将村里所有黄金收归到自己的家里，并按各家上交的黄金数量发给等值的写有字的纸。此时村民就可以拿着这些纸当黄金进行贸易了，而且大家都认得老村长的字，其他人伪造不出来。另外，如果谁的纸磨损太严重，也可拿到老村长那里兑换新的等值的纸，另外老村长承诺任何人如果想要换成真黄金，只要拿纸回来，老村长就会把等值的黄金还给那人。因为老村长写得纸的黄金量和真实放在家里的黄金量是一样的，所以只要严格按照销毁多少纸新写多少纸的原则，每一张有效的纸总能换回相应的真黄金。

此时，比特村进入了符号货币（纸币）时代。而老村长就承担了政府和银行的角色。



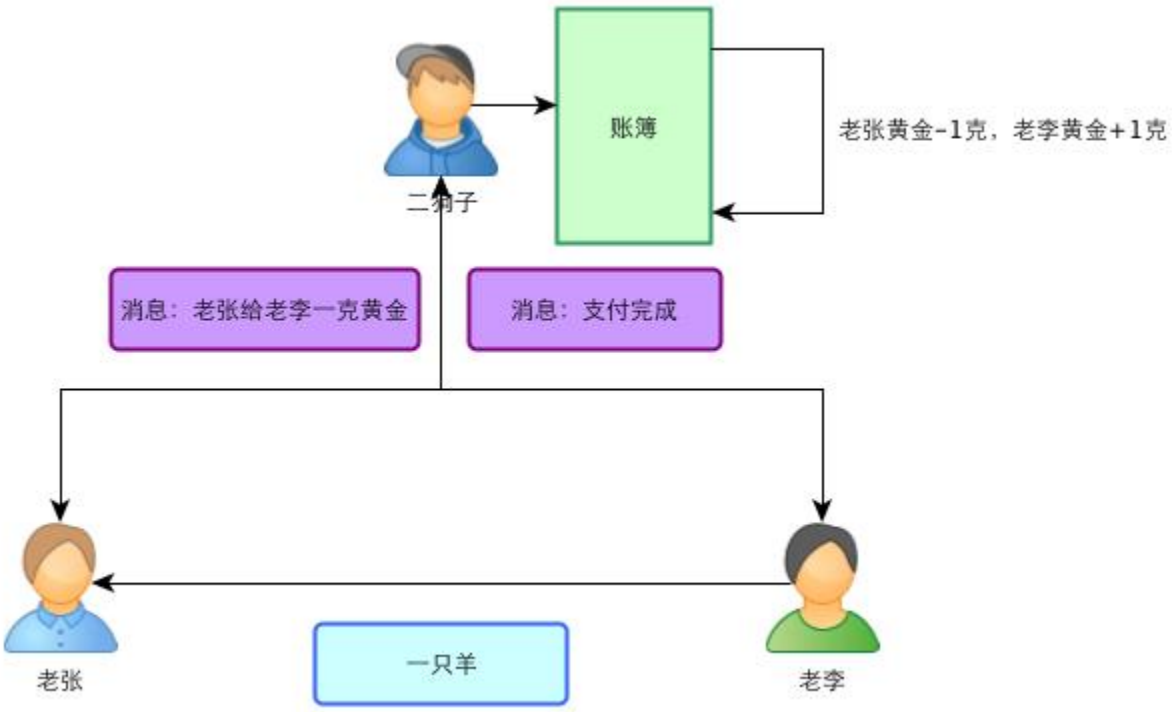
中央系统虚拟货币

又过了几年，老村长由于每天都要核对大量的旧纸币，写新的纸币，还要把各种账目仔细做好记录。一来二去，老村长操劳过度不幸驾鹤西去了。

比特村再次召开全体大会，讨论应该怎么办。此时老村长的儿子二狗子自告奋勇接过了父亲的笔，承担起货币发行的责任。这个年轻的村长二狗子很聪明，他做了几天，发现好像也不用真的写那么多纸。完全可以这样：村民把纸币都交上来，销毁，但是二狗子会记录下每户上交的纸

币数量。以后如果要进行付钱，例如老张要拿一克金子向老李换一只羊，就一起给二狗子打个电话，说明要将老张名下的一克金子划归老李名下，二狗子拿出账本，看看老张名下是否有一克金子，如果有就在老张的名下减掉一克，在老李的名下加上一克，这样就完成了支付，此时老李在电话中听到二狗子确认转账完成，就可以放心让老张把羊牵走了。

此时比特村进入了中央系统虚拟货币时代。每个村民都不需要用实物支付，支付过程变成了二狗子那边维护的账本上数字的变更。



分布式虚拟货币

这新上任的二狗子是聪明，不过这人有时候是聪明反被聪明误。有一天二狗子盯着这账本，心想这全村各户谁有多少钱就是我说的算，那我岂不是……。于是他头脑一热，私自从老张帐下划了十克金子到自己名下。

本以为天衣无缝，但没想到老张也有记账的习惯，有一天他正要付钱却被二狗子告知账户没钱了。老张核对了一下自己的账本，明明还有十克啊，于是拿着账本去找二狗子理论，这一核对发现了那笔未经老张同意的转账。

东窗事发！比特村炸开锅了。二狗子被弹劾是不可避免了，不过通过这件事，大家发现了账本集中在一个人手里的弊端：

- 这个体系完全依赖于账本持有人的个人信用，如果这个人不守规矩，随意篡改账本，那么整个货币系统就会崩溃
- 如果这个人家里失火或者账本失窃，同样也会为整个体系带来毁灭性的打击

正当人们不知所措时，村里一个叫中本聪的宅男科学家走上了台，告诉大家他已经设计了一套不依赖任何中央处理人的叫比特币的虚拟货币系统，可以解决上述问题。然后他缓缓讲述了自己的方案。

下面我们就来看看中本聪同学是如何设计这套系统的。

基础设施搭建

账簿公开机制

中本聪首先说明，要对现有账簿进行如下改造：

1. 账簿上不再记载每户村民的余额，而只记载每一笔交易。即记载每一笔交易的付款人、收款人和付款金额。只要账簿的初始状态确定，每一笔交易记录可靠并有时序，当前每个人持有多少钱是可以推算出来的。
2. 账簿由私有改为公开，只要任何村民需要，都可以获得当前完整的账簿，账簿上记录了从账簿创建开始到当前所有的交易记录。

此言一出，下面立刻炸锅了。第一条还无所谓，但是第二条简直无法接受，因为账簿可是记录了所有村民的交易，这样大家的隐私不全暴露了吗。

中本聪倒是不慌不忙，拿出了一对奇怪的东西。

身份与签名机制（公钥加密系统）

中本聪说，大家不要慌。在他的这套机制下，任何人都不使用真实身份交易，而是使用一个唯一的代号交易。

他展示了手里神奇的东西，说这两件东西分别叫保密印章和印章扫描器。后面他会给村里每一户发一个保密印章和一个印章扫描器。两者的作用如下：

- 保密印章可以在纸上盖一个章，每个印章盖出的章都隐含了一个全村唯一的一串字符，但是凭肉眼是看不出来的。也无法通过观察来制造出相应的印章。

- 印章扫描器可以扫描某个已经盖好的章，读出隐含的信息，并在液晶屏上显示出一串字符。

有了这两个神奇的东西，大家就可以在不暴露真实身份的情况下进行交易了，而印章隐含的那一串字符就是这户人家的代号。具体如何巧妙利用保密印章和印章扫描器进行交易，会在下文详述。

成立虚拟矿工组织（挖矿群体）

下一步，中本聪面向全村招募虚拟矿工，招募要求如下：

- 矿工以组为单位，一组可以是单独的一户，也可以是几户联合为一组
- 成为矿工不影响正常使用货币
- 矿工每天要花费一定时间从事比特币“挖矿”活动，但是不同于挖金矿，虚拟矿工不需要拿着工具去野外作业，在家里就可以完成工作
- 矿工有一定可能性获得报酬，在挖矿活动中付出的努力越多，获得报酬的可能性越大
- 矿工可以随时退出，也可以随时有新的矿工加进来

很快，大约有五分之一的村民加入比特币矿工组织，共分成了 7 个组。

建立初始账簿（创世块）

下面，中本聪宣布，先根据二狗子手里的账簿，把抵押的所有黄金按账簿记录的余额退还给每位村民，然后彻底销毁这本账簿。

然后，中本聪拿出一本新账簿，在账簿的第一页上记录了一些交易记录，特别的是，这些记录的付款人一栏全都是“系统”，而收款人分别是每个印章对应的隐含字符，代表初始时刻，系统为每一户默认分配了一定数量比特币，但是数量非常少，都只有几枚，甚至有些不幸的村户没有获得比特币。

接着中本聪说，由于目前市面上比特币非常少，大家可以先回到用黄金做货币的时代，由于我不是村长，我也没有权利强迫大家一定要承认比特币，大家可以自行决定要不要接受比特币。不过随着比特币的流动和矿工的活动，比特币会慢慢多起来。

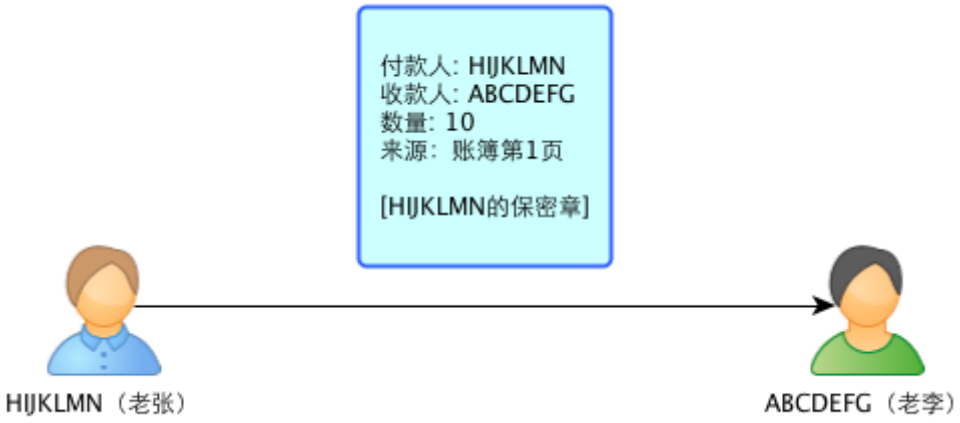
支付与交易

做了这么多铺垫，终于说到重点了，下面说一下在这样一个体系下如何完成支付。以老张付给老李 10 个比特币为例。

付款人签署交易单

为了支付 10 个比特币，老张首先要询问老李的标识字符串，例如是“ABCDEFG”，同时老张也有一个标识字符串例如是“HIJKLMN”，然后老张写一张单子，内容为“HILKLMN 支付 10 比特币给 ABCDEFG”，然后用自己的保密印章改一个章，将这张单子交给老李。另外为了便于追

溯这笔钱的来源，还要在单子里注明这笔钱的来源记在哪一页，例如这个单子里，老张的 10 比特币来自建立账簿时系统的赠送，记录在账簿第一页。



收款人确认单据签署人

老李拿到这个单子后，需要确认这个单子确实是来自“HIJKLMN”这个人（也就是老张）签署的，这个并不困难。因为单子上必须有保密章，老李拿出印章扫描器，扫一下章，如果液晶屏显示出的字符和付款人字符是一致的（这里是“HIJKLMN”），就可以确认单子确实是付款人签署的。这是因为根据保密印章的机制，没有其他人可以伪造印章，任何一个人只要扫描一下印章，都可以确认单子的付款人和盖章人是否一致。

收款人确认付款人余额

这个系统到目前还是很有问题。通过保密印章，收款人虽然可以确认付款人确实签署了这份单子，但是无法自行确认付款人是否有足够的余额支付。之前的中央虚拟货币系统中，二狗子负责检查付款人的余额，并

通知收款人交易是否有效，现在把二狗子开了，谁来负责记账和确认每笔交易的有效性呢？

之前说过，中本聪设计的这个系统是分布式货币系统，不依赖任何中央人物，所以不会有一个或少数几个人负责这件事，最终承担这份工作的是之前所提到的矿工组织。老张、老李和全村其他任何使用比特币进行交易的村民都依赖矿工组织的工作才能完成交易。

矿工的工作

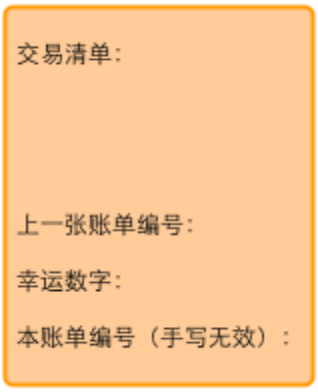
矿工的工作是整个系统的核心，也是最复杂性最高的地方。下面逐步介绍矿工的工作内容和目的。

矿工的工具

俗话说，工欲善其事，必先利其器。比特币矿工虽然不用铁撅、铁锹和探照灯等工具，不过也要有一些必备的东西。

初始账簿。每个组首先自己复制一份初始账簿，初始账簿只有一页，记录了系统的第一次赠送

空账簿纸。每个小组有若干账簿纸，每一页纸上仅有账簿结构，没有填内容，具体内容的书写规则后面讲述。下面是一张空账簿纸的样子，各个字段的意义后面会说到



编码生成器（哈希函数）。中本聪又向矿工组织的每个组分发了若干编码生成器，这个东西很神奇，将一页账簿填好内容的账簿纸放入这个机器，机器会在账簿纸的“本账单编号”一栏自动打印一串由“0”和“1”组成的编号，共 256 个。最神奇的是，编号生成器有如下功能：

- 生成的编号仅与账簿纸上填入的内容有关，与填写人、字体、填写时间等因素均无关
- 内容相同的账簿纸生成的编号总是相同，但是如果内容哪怕只改一个字符，编号就会面目全非
- 编码生成器在打印编码时还需要将所有填入账簿纸的交易单放入，机器会扫描交易单和填入交易单的一致性，尤其是保密印章，如果发现保密印章和付款人不一致，会拒绝打印编码
- 将一张已打印的账簿纸放入，机器会判定编号是否是有效的机器打印，并且判定编号和内容是否一致，这个编号无法伪造
- 交易单收件箱。每个矿工小组需要在门口挂一个箱子用于收集交易单。

- 公告板。每个矿工小组同样需要一个公告板公示一些信息。

有了上面的工具，矿工组织就可以开工了！

收集交易单

中本聪规定，每笔交易的发起人，不但要将交易单给到收款人，还要同时复制若干份一模一样的交易单投递到每个矿工小组的收件箱里。

矿工小组的人定期到自己的收件箱里把收集到的交易单一并取出来。

填写账簿

此时小组的人拿出一张空的账簿纸，把这些交易填写到“交易清单”一栏，同时找到当前账簿最后一页，将最后一页的编号抄写到“上一张账单编号一栏”。 注意还有个“幸运数字”，可以随便填上一个数字，如 12345。然后，将这样账簿纸放入编号生成器，打印好编号，一张账簿就算完成了。

如果你以为矿工的工作就这么简单，那就大错特错了，中本聪有个变态的规定：只有编号的前 10 个数均为 0，这页账簿纸才算有效。

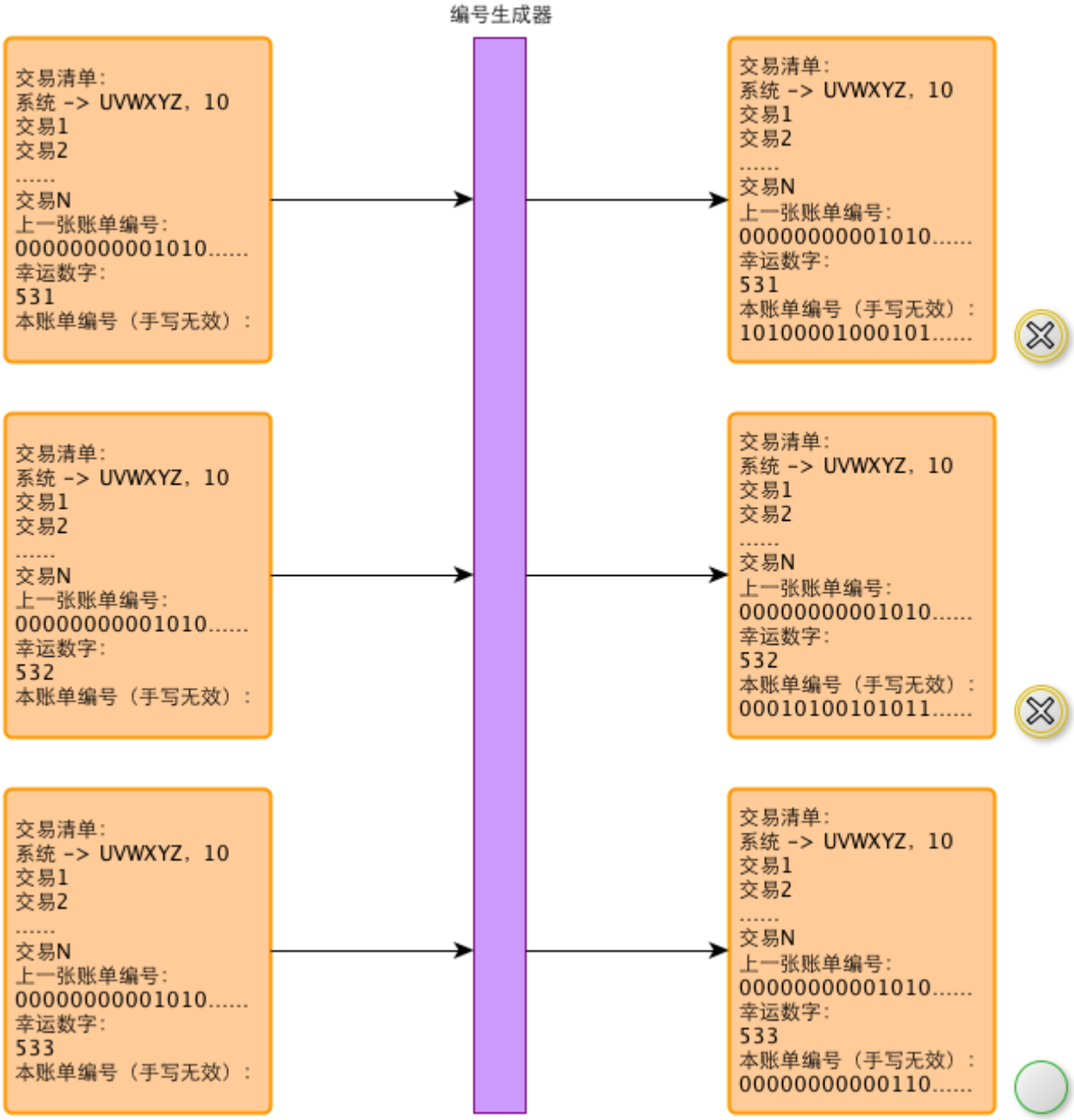
根据之前对编号生成器的描述，要修改编号，只能修改账簿纸的内容，而“交易清单”和“上一张账簿纸编号”是不能随便改的，那么只能改幸运数字了。于是为了生成有效的账簿纸，小组里的矿工就不断抄写账簿纸，但每张纸的幸运数字都不同，然后不断的重复将纸放入编码器，如果生

成的编号不符合规定，这张纸就算废了，重复这个过程直到生成一串有效的编号。

我们知道，如果编号的每一个数字都是随机的，那么平均写 1000 多张幸运数字不同的纸才能获得一个有效的编号。

这就奇怪了，这些矿工为什么要拼命干这看似无意义的事情呢？还记得之前说过矿工有报酬吧，这就是矿工的动力了。中本聪规定：每一张账簿纸的交易清单第一条交易为“系统给这个小组支付 50 个比特币”。也就是说，如果你生成了一张有意义的账簿纸，并且被所有挖矿小组接受了，那么就意味着这条交易也被接受了，你的挖矿小组获得了 50 个比特币。

这就是矿工被叫做矿工的原因，也是为什么之前说随着交易和矿工的活动，比特币的数量会不断增多。例如下面是一个挖矿过程，这个小组的公共比特币帐号为“UVWXYZ”。



在幸运数字尝试到“533”时，系统生成了一页有效账簿。

确认账簿

当某挖矿小组幸运的生成了一张有意义的账簿，为了得到奖励，必须立刻请其它小组确认自己的工作。前面说过，当前村里有 7 个挖矿组，所

以这个小组必须将有效账簿纸誊抄6份快马加鞭送到其他6个小组请求确认。

中本聪规定，当某个小组接到其他小组送来的账簿纸时，必须立即停下手里的挖矿工作进行账簿确认。

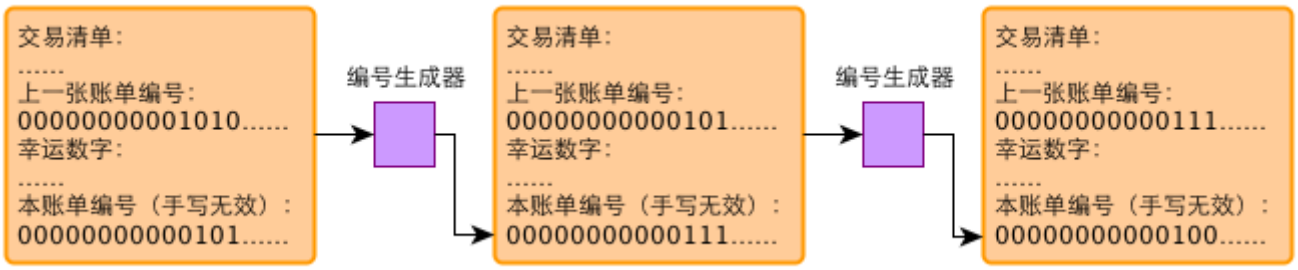
需要确认的信息有三个：

1. 账簿的编号有效
2. 账簿的前一页账簿有效
3. 交易清单有效

首先看第一个，这个确认比较简单。只要将送来的账簿纸放入编码生成器进行验证，如果验证通过，则编号有效。

第二部分需要将账簿页上的“上一页账簿纸编号”和这个小组目前保存的有效账簿最后一页编号比对，如果相同则确认，如果不同，需要顺着已有账簿向前比对，直到找到这个编号的页。如果没有找到指定的“上一页账簿纸编号”对应的页，这个小组会将此页丢掉。不予确认。

注意，由上面的机制可以保证，如果各个小组手里的账簿纸是相同的，那么他们都能按同样的顺序装订成相同的账簿。因为后面一张纸的编号总是依赖前面的纸的编号，编码生成器的机制保证了所有合法账簿纸的相对先后顺序在每个小组那里都是相同的（可能会有分支，但不会出现环，后面细讲）。



最后是如何确认交易清单有效，其实也就是要确认当前每笔交易的付款人有足够的余额支付这笔钱。由于交易信息里包含这笔钱是如何来的，还包含了记录来源交易的账单编号。例如，HIJKLMN 要给 ABCDEFG10 个比特币，并注明了这 10 个比特币来自之前 OPQRST 支付给 HIJKLMN 的一笔交易，确认时首先要确认之前这笔交易是否存在，同时还要检查 HIJKLMN 在这之前没有将这 10 个比特币支付给别人。这一切确认后，这笔交易有效性就被确认了。

其中第一笔是系统奖励给生成这页账簿的小组的 50 个，这笔交易大家都默认承认，后面的只要按照上述方法追溯，就可以确认 HIJKLMN 是否当前真有 10 个比特币支付给 ABCDEFG。

如果完成了所有了上述验证并全部通过，这个小组就认可了上述账簿纸有效，然后将这张账簿纸并入小组的主账簿，舍弃目前正在进行的工作，后面的挖矿工作会基于这本更新后的主账本进行。

账簿确认反馈

对于挖矿小组来说，当账簿纸送出去后，如果后面有收到其他小组送来的账簿纸，其“上一页账簿纸编号”为自己之前送出去的账簿纸，那么就

表示他们的工作成功被其他小组认可了，因为已经有小组基于他们的账簿纸继续工作了。此时，可以粗略的说可以认为已经得到了 50 个比特币。

另外，任何一个小组当新生成有效账簿纸或确认了别的小组的账簿纸时，就将最新被这个小组承认的交易写到公告牌上，那么收款人只要发现相关交易被各个小组认可了，基本就可以认为这笔钱已经到了自己的账上，后面他就可以在付款时将钱的来源指向这笔交易了。

以上就是整个比特币的支付体系。下面我们来分析一下，这个体系为什么可以工作下去，以及这个体系可能面临的风险。

工作机制分析

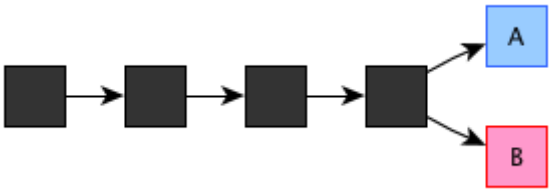
虽然上面阐述了比特币的基本运作规则，但是村民们还是有不少疑问。所以中本聪同学专门开了个答疑会，解答常见问题。下面总结一下村民最集中关心的问题。

核心问题答疑

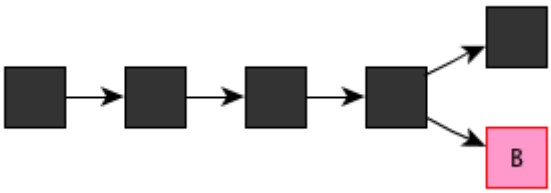
如果同时收到两份合法的账簿页怎么办？

注意在上面的运行机制中，各个挖矿小组是并行工作的，因此完全可能出现这样的情况：某小组收到两份不一样的账簿页，它们都基于当前这个小组的主账簿的最后一页，并且内容也都完全合法，怎么办？

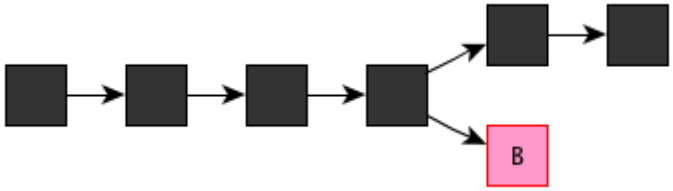
关于这个问题，中本聪同学说，小组不应该以线性方式组织账簿，而应该以树状组织账簿，任何时刻，都以当前最长分支作为主账簿，但是保留其它分支。举个例子，某小组同时收到 A、B 两份账簿页，经核算都是合法的，此时小组应该将两页以分叉的形式组织起来，如下图所示：



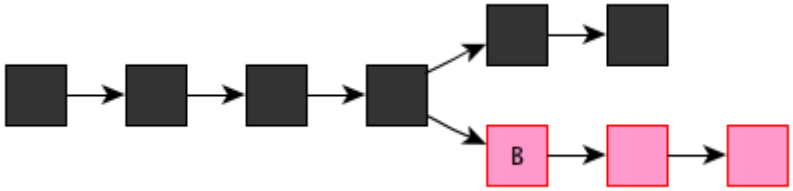
黑色表示当前账簿主干。此时，可以随便选择一个页作为当前主分支，例如选择 A：



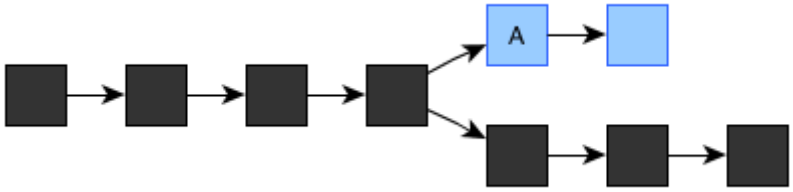
此时如果有一个新的账簿页是基于 A 的，那么这个主干就延续下去：



如果这个主干一直这么延续下去，表示大家基本都以 A 为主干，B 就会被遗忘。但是也有可能忽然 B 变成更长了：



那么我们就需要将 B 分支作为当前主干，基于这个分支进行后续工作。



从局部来看，虽然在某一时刻各个小组的账簿主干可能存在不一致，但大方向是一致的，那些偶尔由于不同步产生的小分支，会很快被淹没在历史中。

如果挖矿小组有人伪造账簿怎么办

关于这个问题，中本聪同学说，只要挖矿组织中大多数人是诚实的，这个系统就可靠，具体分几个方面给予答复。

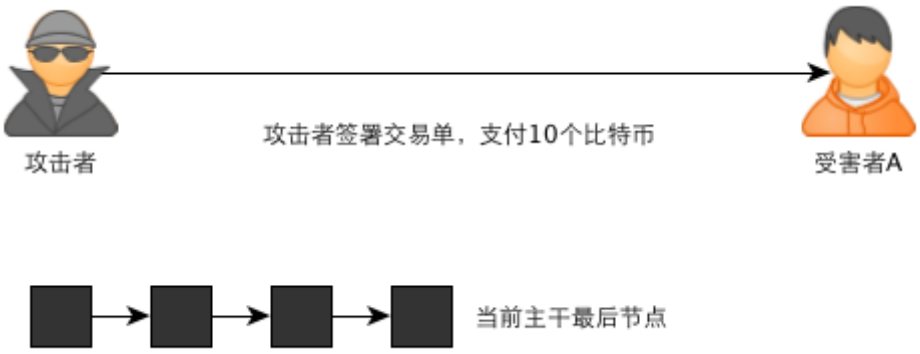
首先，基于保密印章机制，没有人能伪造他人身份进行付款，因为编码生成器在打印编码时会核对所有交易单的保密印章，印章和付款人不一致会拒绝打印。

而且诚实的矿工也不会承认不合法的交易（如某笔交易付款方余额不够）。

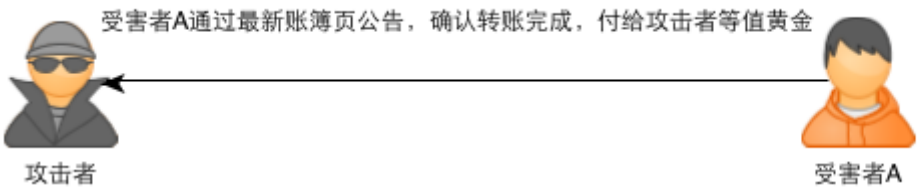
所以只有一种可能的攻击行为，即在收款人确认收款后，从另一条分支上建立另外的交易单，取消之前的付款，而将同一笔钱再次付款给另一个人（即所谓的 double-spending 问题）。下面同样用一个例子说明这个问题。

先假设有一个攻击者拥有 10 个比特币，他准备将这笔钱同时支付给两名受害者 A 和 B，并都得到承认。

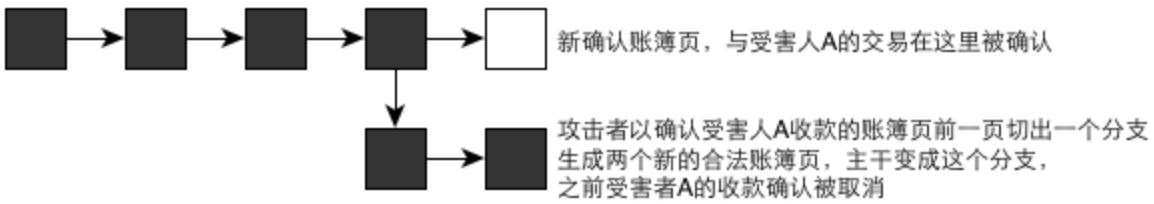
第一步，攻击者准备从受害者 A 手里买 10 比特币的黄金，他签署交易单给受害者 A，转 10 个比特币给受害者 A。



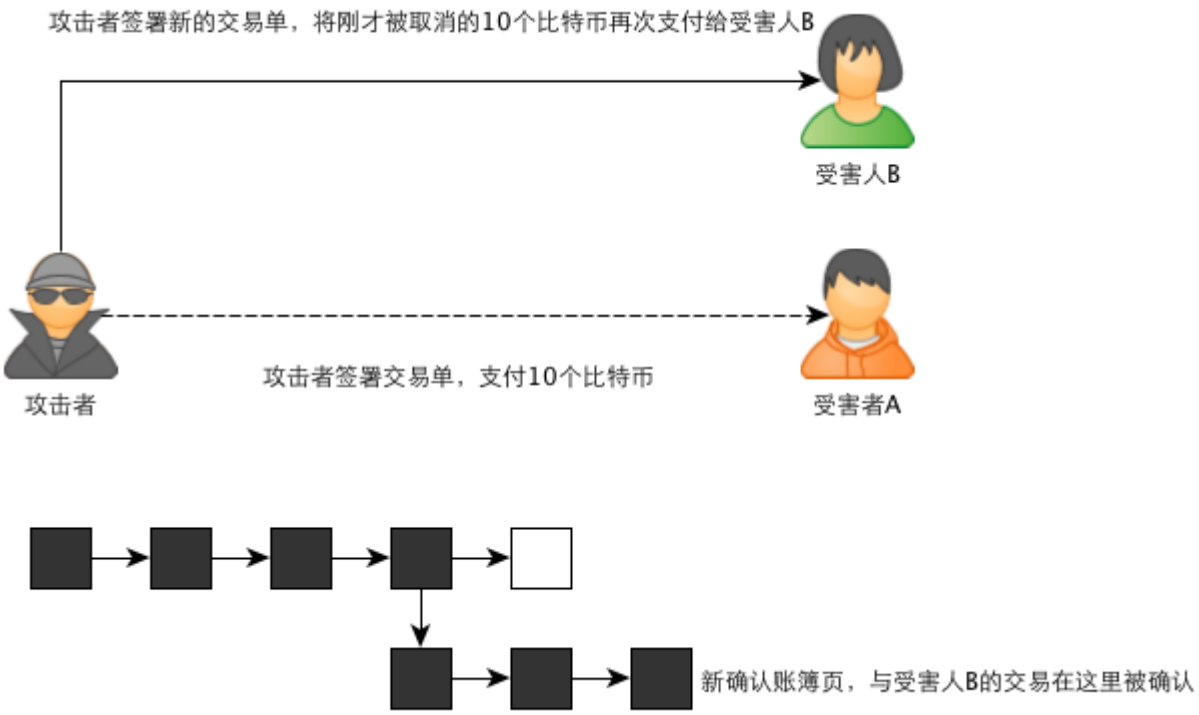
第二步，这笔交易在最新的账簿页中被确认，并被各个挖矿小组公告出来。受害人 A 看到公告，确认比特币到账，给了攻击者 10 个比特币等值的黄金。



第三步，攻击者找到账簿，从包含刚才交易的账簿页的前一页做出一个分支，生成更多的账单页，超过刚才的分支。由于此时刚才攻击者制造的分支变成了主干分支，而包含受害者 A 得到钱的分支变成了旁支，因此挖矿组织不再承认刚才的转账，受害者 A 得到的 10 比特币被取消了。



第四步，攻击者可以再次签署交易单，将同一笔钱支付给受害者 B。受害者 B 确认钱到账后，支付给攻击者等值黄金。



至此，攻击者将 10 个比特币花了两次，从两名受害者那里各购得等值黄金。攻击者还可以如法炮制，取消与受害者 B 的转账，将同一笔钱再支付给其他人……

关于这种攻击，中本聪给出的解决方案是，建议收款人不要在公告挂出时立即确认交易完成，而是应该再看一段时间，等待各个挖矿小组再挂出 6 张确认账簿，并且之前的账簿没有被取消，才确认钱已到账。

中本聪解释道，之前设定变态的编号规则，正是为了防御这一点。根据前面所述，生成有效账簿页不是那么简单的，要花费大量的人力反复试不同的幸运数字，而且过程完全是碰运气。如果某账簿页包含你收到钱的确认，并且在后面又延续了 6 个，那么攻击者想要在落后 6 页的情况

下从另一个分支赶超当前主分支是非常困难的，除非攻击者拥有非常多的人力，超过其他所有诚实矿工的人力之和。

而且，如果攻击者有如此多人力，与其花这么大力气搞这种攻击，还不如做良民挖矿来的收益大。这就从动机上杜绝了攻击的形成。

比特币会一直增加下去，岂不是会严重通货膨胀

中本聪说，这一点我也想到了。前面忘了说了，我给矿工组织的操作细则手册会说明，刚开始我们协议每生成一页账簿，奖励小组 50 个比特币，后面，每当账簿增加 21,000 页，奖励就减半，例如当达到 210,000 页后，每生成一页账簿奖励 25 个比特币，420,000 页后，每生成一页奖励 12.5 个，依次类推，等账簿达到 6,930,000 页后，新生成账簿页就没有奖励了。此时比特币全量约为 21,000,000 个，这就是比特币的总量，所以不会无限增加下去。

没有奖励后，就没人做矿工了，岂不是没人帮忙确认交易了

到时，矿工的收益会由挖矿所得变为收取手续费。例如，你在转账时可以指定其中 1%作为手续费支付给生成账簿页的小组，各个小组会挑选手续费高的交易单优先确认。

矿工如果越来越多，比特币生成速度会变快吗

不会。中本聪解释，虽然可以任意加入和退出矿工组织，导致矿工人数变化，每个矿工也会拿到一个编码生成器，不过我已经在编码生成器中

加入了调控机制，当前工作的编码生成器越多，每个机器的效率就越低，保证新账簿页生成速率不变。

虽然每个人的代号是匿名的，但如果泄露了某个人的代号，账簿又是公开的，岂不是他的所有账目都查出来了

确实是这样的。例如你要和某人交易，必然要要到他的代号才能填写交易单。因为收款人一栏要填入那人的代号。不过中本聪说可以提供无限制的保密印章，建议每一次交易用不同的保密印章，这样查账簿就追查不到同一个人的所有账目了。

答疑完毕。